# CALIFORNIA PUBLIC EMPLOYEES' RETIREMENT SYSTEM

Management Comments and Recommendations

For the Year Ended June 30, 2008

**DRAFT**

**CALIFORNIA PUBLIC EMPLOYEES' RETIREMENT SYSTEM**

**Management Comments and Recommendations**

**For the Year Ended June 30, 2008**

**TABLE OF CONTENTS**


Page(s)

Transmittal Letter..... 1-2

Management Comments and Recommendations..... 3-11

Status of Prior Year Recommendations..... 12-29


**DRAFT**

November 20, 2008

To the Finance Committee of the
California Public Employees' Retirement System
Sacramento, California

In planning and performing our audit of the financial statements of the California Public Employees' Retirement System (CalPERS) as of and for the year ended June 30, 2008, in accordance with auditing standards generally accepted in the United States of America, we considered CalPERS' internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of CalPERS' internal control. Accordingly, we do not express an opinion on the effectiveness of CalPERS' internal control.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or a combination of control deficiencies, that adversely affects CalPERS' ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of CalPERS' financial statements that is more than inconsequential will not be prevented or detected by CalPERS' internal control.

A material weakness is a significant deficiency, or a combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by CalPERS' internal control.

Our consideration of internal control was for the limited purpose described in the first paragraph and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. We did not identify any deficiencies in internal control that we consider to be material weaknesses, as defined above.

During our current and prior audits, we became aware of several matters that are opportunities for strengthening internal controls and operating efficiency. The current year comments are included in the Management Comments and Recommendations section; the status of prior year comments is included in the Status of Prior Year Recommendations section of this report.

CalPERS' written responses to the recommendations identified in our audit are described in the Management Comments and Recommendations and the Status of Prior Year Recommendations sections. We did not audit the responses and, accordingly, we express no opinion on them.

We would like to thank CalPERS management and staff for the courtesy and cooperation extended to us during the course of our engagement.

The accompanying management comments and recommendations and status of prior year recommendations are intended solely for the information and use of the Board of Administration, Finance Committee, management and others within CalPERS and are not intended to be and should not be used by anyone other than these specified parties.

Certified Public Accountants
Sacramento, California
November 20, 2008

## ACCOUNTING AND RECONCILIATION PROCEDURES

### Accounting for Service Credit Purchases

**Observation #1** Certain members of CalPERS are eligible to purchase service credits to increase future retirement benefits. The cost to purchase service credits is based on formulas established by law and varies based on the amount of service credits purchased and the membership type. Payment options include installment agreements with terms up to 180 months. Fiscal Services currently records receivables for purchased service credits and recognizes the related contributions when the installment payments are received. Generally accepted accounting principles (GAAP) require that service credit purchases be recorded as receivables and recognized as contributions upon execution of the agreement. GAAP further requires that receivables be recorded at their net realizable value, which is the net amount expected to be collected under the agreements.

We recommend that Fiscal Services properly record service credit purchases under installment agreements in accordance with GAAP. Contributions should be recognized at the time the installment agreement is executed, rather than deferred until payment is received. Fiscal Services should also analyze prior repayment patterns and estimate an allowance for doubtful accounts to record receivables at their net realizable value.

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will review and implement procedures to recognize service credit purchase contributions in accordance with GAAP. Fiscal Services will work with the Member Services Division to analyze prior repayment patterns and record a fiscal year end entry to estimate an allowance for doubtful accounts to state these receivables at their net realizable value.

### Accounting for Real Estate Investments

**Observation #2** CalPERS' Investment Accounting - Real Estate Unit records real estate investment transactions based on the monthly or quarterly financial statements submitted by real estate partners. The real estate partners also submit year-end audited financial statements. The Real Estate Investment Unit within Fiscal Services does not reconcile the partners' audited financial statements to CalPERS' general ledger or the partners' monthly or quarterly financial statements, which increases the risk that adjustments made during the partnership audit are not properly reflected in the general ledger.

In addition, we identified one real estate partner that had not submitted audited financial statements in a timely manner. The most recent audited financial statements were issued October 13, 2008, for the period ended December 31, 2007. Partnership agreements require partners to submit audited financial statements within 120 days of the partnership's year-end. There is currently no process in place to monitor the submission of the audited financial statements.

**Observation #2 - Accounting for Real Estate Investments (Continued)**

We recommend that management establish a formal policy requiring the reconciliation of the partnerships' audited financial statements with CalPERS' general ledger or partnerships' monthly or quarterly financial statements. Differences, if any, should be evaluated to determine whether the general ledger accurately reflects real estate transactions and balances. Furthermore, management should implement a formal process to monitor the receipt of audited financial statements and ensure partners comply with contract provisions.

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will work with the Investment Office to establish a formal policy requiring the reconciliation of the partnerships' audited financial statements with CalPERS' general ledger or partnerships' monthly or quarterly financial statements. Fiscal Services will also implement a reconciliation process that will compare the audited financial statements with the monthly or quarterly financial statements reported by the real estate partners for the same period using the new automated real estate investment system (AREIS). Any discrepancies noted will be brought to the attention of the Investment Office and the real estate partners for explanation or adjustment.

**Master Reconciliation – Public Employees' Retirement Fund**

**Observation #3** Fiscal Services prepares the Master Reconciliation, which reconciles investment transactions recorded in the general ledger system with the transactions recorded by CalPERS' custodian bank. We identified 2 reconciling items, totaling approximately $26.9 million, in the June 2008 Master Reconciliation that had not been investigated and resolved in a timely manner. The reconciling items, which were described as fiscal year 2004 performance and management fees, have been carried forward from prior years. Timely resolution of reconciling items is an essential part of the accounting function.

We recommend that Fiscal Services investigate and resolve all discrepancies as part of the reconciliation process. Reconciling items should not be carried forward to future periods unless they represent legitimate timing differences.

**Management Response:**

Fiscal Services concurs with the recommendation. The two outstanding reconciling items on the June 2008 Master Reconciliation from fiscal year 2004 for performance and management fees have been investigated and resolved as of December 2008. Fiscal Services will enhance our Master Reconciliation processes and procedures to clear reconciling items timely and mitigate reconciling items from being carried forward to future periods unless they represent legitimate timing differences. An aging report will be developed and implemented to monitor, address, and timely clear reconciling items and further enhance management's oversight of the Master Reconciliation report processes.

## Account Reconciliations - Deferred Compensation Fund

**Observation # 4** The Deferred Compensation Fund (DCF) acts as a paying agent for CalPERS' supplemental income plans. In performing our audit procedures, we discovered several errors in the DCF, as Fiscal Services had not reconciled year-end account balances. Management recorded several audit adjustments to correct revenues, expenses and liabilities as a result of our procedures.

We recommend that Fiscal Services develop a formal policy that requires a periodic analysis and reconciliation of DCF account balances.

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will develop a formal policy that requires a periodic analysis and reconciliation of DCF account balances. Fiscal Services will also review and enhance the current general ledger account structure in the DCF. These improvements will mitigate miscoding of revenue, expenses and liabilities, and increase management oversight of more timely account balance reconciliations.

## Allocation of Investment Balances – Supplemental Contributions Program and IRC 457 Funds

**Observation # 5** During fiscal year 2008, CalPERS expanded the investment options in the Supplemental Contributions Program (SCP) to include each of the 18 investment options provided in the IRC 457 plan. Although the third party administrator maintains records of individual participant accounts, the custodian bank does not account for the investments of the SCP and IRC 457 in separate portfolios. As a result, for financial statement purposes, Fiscal Services manually allocated the investment balances and the related investment receivables, payables, gains and losses based on the ratio of the respective asset and liability accounts within a portfolio which contains holdings of both funds reported by the custodian bank. The manual allocation increases the risk that investment–related activities will be misstated in the financial statements.

We recommend that management consider whether the current practice of allocating investment balances and related investment receivables, payables, gains and losses is adequate or whether the custodian bank should maintain separate investment portfolios for the supplemental income plans in order to avoid the manual process.

**Management Response:**

Fiscal Services concurs with the recommendation. The multi-class structure of Supplemental Income Plan (SIP) portfolios established by the custodian bank does not accommodate separate investment portfolios for each plan (IRC-457 and SCP). Fiscal Services will work with the custodian bank to provide CalPERS with customized reporting that will eliminate the manual calculation processes and segregate financial data such as investment balances and related investment receivables, payables, gains and losses by plan.

## FINANCIAL REPORTING

### Investment Disclosures

**Observation #6** Fiscal Services utilizes investment data provided by the custodian bank to prepare the financial statement disclosures required by Governmental Accounting Standards Board (GASB) Statement No. 40, *Deposit and Investment Risk Disclosures – an amendment of GASB Statement No. 3*. Our audit procedures revealed numerous errors and inconsistencies in the disclosures, as Fiscal Services did not independently verify whether the amounts provided by the custodian bank were accurate or in conformity with the provisions of GASB Statement No. 40. The original data provided by the custodian bank had a variance of approximately $6 billion which was subsequently addressed and the appropriate data was included in the CalPERS financial statements. Furthermore, Fiscal Services did not ensure that the custodian bank provided the underlying data in a timely manner, which created challenges in meeting the audit deadline.

We also discovered errors in the financial statement disclosure of unfunded alternative investment commitments. Certain amounts provided by CalPERS' third party service provider did not agree to information provided by the partners. Although the disclosed amounts were corrected, Fiscal Services did not independently corroborate the unfunded commitments in preparing the financial statement disclosure.

We recommend that Fiscal Services reconcile GASB Statement No. 40 investment data provided by the custodian bank with the general ledger to validate the accuracy and completeness of the data. Fiscal Services should also perform procedures to ensure the conformity of the related disclosures with GAAP reporting requirements. Deadlines should be clearly established with the custodian to allow sufficient time for internal review and external audit procedures. We further recommend that Fiscal Services compare unfunded alternative investment commitment amounts provided by the third party service provider to the related partnership financial statements to determine that amounts are complete and calculated correctly.

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will reconcile GASB Statement No. 40 investment data to the general ledger and will follow up on any discrepancies with the custodian bank. Fiscal Services will also develop and perform procedures to ensure the conformity of the related disclosures with GAAP reporting requirements.

Fiscal Services implemented a quarterly reconciliation process in fiscal year 2008-09 to compare the unfunded amounts reported by the general partner with those reported by PrivateEdge, third party service provider. The reconciliation will be reviewed to determine that the amounts are complete and calculated correctly and any discrepancies noted are brought to the attention of PrivateEdge for explanation or correction.

Furthermore, Fiscal Services will work with the Investment Office, who manages the contracts for both the service provider and master custodian, to improve the reports provided by the service provider to be in accordance with GAAP guidelines.

## Preparation of Trial Balances and Audit Readiness

**Observation #7** Subsequent to providing the independent auditor with the June 30, 2008 trial balances, Fiscal Services recorded approximately 60 journal entries, which changed the account balances and transaction totals in numerous funds. Because the auditor utilizes the trial balances to determine sample sizes, conduct tests of details, and perform analytical procedures, the changes created considerable inefficiencies in the audit process for both Fiscal Services and the auditor, which resulted in added costs for CalPERS. The significant number of journal entries resulted from untimely reconciliations and closing procedures, as well as the timing of information received from third parties.

We recommend that Fiscal Services assess its resources and existing workload in order to establish a reasonable timeline for closing the books and preparing the trial balances. Trial balances provided to the auditor should reflect all accruals, adjustments and closing journal entries other than certain adjustments for real estate and private equity investments which are dependent upon information provided by third parties.

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will assess its resources, existing workload, and current procedures in order to develop a reasonable timeline for closing the books and preparing the trial balances. Fiscal Services will incorporate procedures to ensure reconciliations are completed timely to ensure the trial balances provided to the external auditors will reflect all accruals, adjustments, and closing journal entries other than certain adjustments for real estate and private equity investments which are dependent upon third party information.

## Observation #8 - Evaluation of Contingencies

Our audit procedures include inquiries of CalPERS' general counsel as well as outside attorneys regarding pending litigation, claims and assessments. GAAP requires that contingent losses be accrued for matters in which a material loss is probable and reasonably estimable. If both of these conditions have not been met, contingent losses must be disclosed when it is at least reasonably possible that a loss may have been incurred. In the attorneys' responses, we identified a contingent loss that was not properly disclosed in the draft financial statements. Although Fiscal Services updated the note disclosures to reflect the contingency, current procedures are not sufficient to ensure that contingencies will be accrued or disclosed in accordance with GAAP.

We recommend that Fiscal Services meet with CalPERS' general counsel to identify pending litigation, claims and assessments in conjunction with the preparation of the annual financial statements. In addition, Fiscal Services should review all legal responses to the auditor's inquiries and determine whether matters must be accrued or disclosed in the financial statements.

**Observation #8 - Evaluation of Contingencies (Continued)**

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will coordinate efforts with CalPERS' General Counsel to develop a process where Fiscal Services will be notified of pending litigation, claims and assessments in conjunction with the preparation of the annual financial statements. In addition, Fiscal Services will review the responses to the auditor's inquiries provided by CalPERS' Legal Office as well as outside attorneys and determine whether there are material items which must be accrued or disclosed in the financial statements.

**Management's Discussion and Analysis**

**Observation #9** Fiscal Services prepares management's discussion and analysis (MD&A), which includes a discussion of the reasons for changes in financial position and results of operations in the current year compared to the prior year. MD&A prepared by Fiscal Services meets the minimum GAAP requirements; however, we believe incorporating the unique perspectives of the managers responsible for key activities would enhance the usefulness and improve the users' understanding of the financial statements. Appropriate personnel in the Investment Office, Benefit Services Division, and Health Benefits Branch, at a minimum, should be involved in the preparation of MD&A and should provide the reasons for changes and known facts, conditions, or decisions that are expected to have a significant effect on the financial position or results of operations.

We recommend that Fiscal Services obtain narrative explanations of the significant changes in financial position and results of operation from management responsible for the related activities. Fiscal Services should be heavily involved in the analysis to ensure compliance with the financial reporting standards and to avoid redundancy in the MD&A.

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will lead the CalPERS Financial Reporting Committee to meet these objectives. The Committee is attended by representatives from each Branch, the Office of Audit Services, and the Assistant Executive Officer of the Administrative Services Branch to discuss financial reporting enhancements and the implication of program changes on financial reporting. As the coordinator and facilitator for the Committee, Fiscal Services will add this observation to the agenda of the next CalPERS Financial Reporting Committee. Key individuals, who will provide the narrative, will be identified and provided with guidelines for developing explanations of significant changes in financial position and results of operations that conform to the GASB 34 directives, which establishes the financial reporting standards for the MD&A of state and local governments.

## CONTROLS OVER BENEFIT PAYMENTS

### IRC 415 Compliance Procedures - Replacement Benefits Fund

**Observation #10** Internal Revenue Code (IRC) Section 415(b) limits the annual benefits that can be accrued or paid to a member of a qualified defined benefit pension plan. IRC 415(b) dollar limits are established each year by the IRS and vary based on the retirement age of participants. CalPERS utilizes the Replacement Benefits Fund to account for the collection of employer contributions and the related payment of benefits equivalent to amounts that exceed the IRC 415 dollar limits. Currently, a spreadsheet designed by the Actuarial and Employer Services Branch is used to calculate replacement benefits. The spreadsheet is not password protected; as a result, authorized personnel having access to the worksheet can accidentally delete a formula or cell value within the worksheet. In addition, one employee is responsible for calculating replacement benefit payments, sending notification letters to the applicable members, and preparing the employer invoices. Existing policies do not require management review of these procedures.

The Actuarial and Employer Services Branch should establish a password for the spreadsheet used to calculate replacement benefits, and only personnel with responsibility for the calculations should be given the password. Certain formula or cell value within the worksheet should be protected to prevent unauthorized modification. In addition, management should establish a formal policy requiring an independent review of the calculations, member notification letters and employer invoices prior to disbursement.

**Management Response:**

The Actuarial Office will work with the Benefit Services Division (BNSD) to implement a password protected spreadsheet in the 2009 calendar year. Certain formula or cell values within the worksheet will be protected to prevent unauthorized modification. In addition, a formal policy will be developed by BNSD to ensure the calculations, notification letters and invoices are regularly reviewed.

## PAYMENT OF INVESTMENT AND ADMINISTRATIVE EXPENSES - IRC 457, SPOF AND SCP FUNDS

**Observation #11** Administrative and investment management fees for the IRC 457 fund, State Peace Officers' and Firefighters fund (SPOFF) and the Supplemental Contributions Program fund (SCPF) are calculated by the custodian bank, and are not independently validated by Fiscal Services staff prior to posting to the general ledger and payment. During fiscal year 2008, CalPERS was billed twice for the same services, which resulted in excess transfers of approximately $584,000 from the IRC 457 and $1.8 million from the SPOFF to the DCF (paying agent). In addition, we noted a delay in receiving invoices from third parties for the administrative and management functions. As a result, the fourth quarter invoices recorded in the CalPERS financial statements were based on estimates.

**Observation #11 – Payment of Investment and Administrative Expenses - IRC 457, SPOF and SCP Funds (Continued)**

We recommend that Fiscal Services independently verify fees calculated by the custodian bank prior to posting to the general ledger and payment and ensure timely receipt of invoices from third parties.

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will implement procedures to verify fees calculated by the custodian bank prior to posting to the general ledger. Fiscal Services will also work with the Investment Office to ensure these invoices are received as soon as possible and independently verify fees presented on invoices received from third parties prior to payment.

## ACTUARIAL ASSUMPTION - JUDGES RETIREMENT FUND

**Observation #12** The June 30, 2007 actuarial valuation for the Judges Retirement Fund (JRF) assumes a 7 percent investment rate of return in calculating the plan liabilities and the State of California's (State's) annual required contributions. The State has a pattern of funding benefits as they become due. As a result, the JRF has not accumulated significant long-term investments for the payment of future benefits. GASB No. 25 sets forth the parameters for actuarial data presented in the note disclosures and required supplementary information. Those standards state "the investment return assumption should be based on an estimated long-term investment yield for the plan with consideration given to the nature and mix of current and expected plan investments…" Although guidance for plans that do not accumulate significant long-term investments is not explicit in GASB No. 25, financial reporting standards governing other postemployment benefit plans indicate the investment rate of return should be consistent with the employers investment yield if the plan has no assets.

We recommend that CalPERS Actuarial Office consider whether the current 7% rate of return assumption is appropriate for financial reporting purposes, given the short-term nature of JRF assets. The Actuarial Office should consider whether a lower interest rate, consistent with the expected yield of the State's short-term investments, would be more appropriate.

**Management Response:**

Beginning with the June 30, 2008 actuarial valuation, CalPERS Actuarial Office will disclose financial reporting numbers based on a lower interest rate, consistent with the expected yield of the State's short-term investments. To ensure consistency, the interest rate selected should be the same as the interest rate used for the pay-as-you go scenario in the OPEB actuarial valuation report issued by the State Controller's Office covering the same fiscal year as the fiscal year of the ARC for JRF. However, CalPERS will continue to provide in its actuarial valuation report figures using the 7 percent investment rate in the event the State decided to start pre-funding benefits.

## ELECTRONIC DATA PROCESSING PASSWORD POLICY

**Observation #13** During our review of electronic data processing policies, we found that password requirements used to access the mainframe applications, RIBS and CRS, currently do not fully adhere to CalPERS' Information Security Identity Authentication Practice in the following areas:

| *Configuration* | *Mainframe Settings* | *I.S. Identity Authentication Practice* |
|---|---|---|
| *Password length* | *6-8 characters* | *8 characters* |
| *Minimum password age* | *0* | *1 day* |
| *Password Complexity* | *not required* | *complex passwords required* |

We recommend CalPERS' mainframe administrator should update the Resource Access Control Facility (RACF) security settings to ensure that the settings comply with the Information Security Identity Authentication Practice. The Information Security Office should conduct periodic monitoring to ensure compliance.

**Management Response:**

The Enterprise Mainframe Service Support Team (the Team) agrees with the finding and recommendation. The mainframe RACF administrators and Enterprise Mainframe Server Support technical staff will update the RACF security settings to insure that they comply with the ISOF Identity Authentication Practice. The Team plans to start this effort immediately after the upgrade of our mainframe operating system that is being implemented on September 28, 2008. The planned target completion date is January 31, 2009.

## INVESTMENT ACCOUNTING

### Real Estate Accounting and Reporting

### Investment Office, Performance Monitoring Unit

**Prior Year Observation #1** Real estate investment values are derived from independent appraisals when called for by Policy and real estate partnership financial statements. Based on our testing of real estate appraisals, internal controls are not sufficient to ensure that appraised values of real estate investments covered by the CalPERS Investment Policy for Equity Real Estate Appraisal and Valuation are properly recorded by the related partnership. CalPERS established a Performance Monitoring Unit (PMU) in the Investment Office's Administrative Services and Operations Unit. The PMU's responsibility includes selecting appropriate appraisers and finalizing the valuations with the related partnerships, but does not include verifying that appraised values are properly incorporated in the partnership financial records.

We recommend that management implement procedures to ensure that appraised values are properly recorded by the related partnership which should include correlation of appraised property to the partnership financial statements.

**Management Response:**

Management agrees with the recommendation to implement procedures to ensure that those real estate assets that are appraised subject to Policy are properly recorded by the related partnership.

**Current Year Status:**

During the fiscal year 2008 audit, PMU developed a process to verify that real estate assets were reasonably reported at appraised values for core real estate. However, we recommend that the same process be completed for non-core real estate properties. PMU should implement procedures to ensure that fair market value of appraised non-core real estate assets are reasonably reported by the partners. In addition, sufficient time should be given for the external auditors to review the work performed and re-perform the procedures on a sample basis.

Investment Office (INVO) agrees with the current year status. INVO will continue to enhance its internal procedures to verify that the appraised value of assets is being reasonably reported by non-core real estate partnerships in their financial statements. In addition, INVO will continue its development of a technology-based solution that may assist the external auditor perform their review in a more time-efficient manner.

**Fiscal Services Division, Investment Accounting Unit**

**Prior Year Observation #2** We also noted that real estate investment records utilized by the Performance Monitoring Unit (PMU) do not directly correlate with data maintained by Fiscal Services Division's Real Estate Investment Accounting Unit, which increases the risk of errors in the financial reporting process.

We recommend that Fiscal Services Division reconcile quarterly its records in the General Ledger accounts with the records maintained by the PMU of the Investment Office.

**Management Response:**

Fiscal Services concurs with the recommendation. The Real Estate Investment Accounting Unit has modified the General Ledger Posting Templates used to post partnership financial activity. The General Ledger Posting Templates will include a quarterly reconciliation which will then be compared with the PMU data. Differences, if any, will be investigated and the appropriate adjustments to the General Ledger or PMU reports will be made.

**Current Year Status:**

The recommendation has been implemented.

**Real Estate Contributions and Distributions Accounts**

**Prior Year Observation #3** Real estate contribution and distribution accounts capture cash flow transactions relating to real estate investments. Balances in these clearing accounts typically represent timing differences between State Street Bank records and real estate partnership financial statements. During the fiscal year ended June 30, 2007, Fiscal Services had not sufficiently reconciled the balances. As a result, CalPERS recorded an audit reclassification of approximately $628 million to correct the resulting overstatement of real estate income and expenses.

We recommend that current accounting practices should be evaluated to ensure that real estate contribution and distribution accounts are sufficiently analyzed and related transactions and balances are properly recorded as part of the ongoing accounting function.

**Management Response:**

Fiscal Services concurs with the recommendation. As part of the Accounting Action Plan 2007 efforts, Fiscal Services is now reconciling the real estate contribution and distribution control accounts on a monthly basis. The reconciling items are identified by partner and will be sufficiently analyzed and recorded.

**Current Year Status:**

The recommendation has been implemented.

## Real Estate Insurance Premiums

**Prior Year Observation #4** To obtain the most favorable insurance rates, CalPERS purchases property insurance for all real estate investments. The partnership holding the real estate investment is required to reimburse CalPERS for insurance premium payments. During the fiscal year ending June 30, 2007, insurance premiums paid by CalPERS were not tracked and monitored to ensure the respective partnerships properly reimbursed CalPERS. In addition, we noted several partnerships submitted reimbursements directly to Real Estate Investment Accounting rather than the CalPERS Cashier Unit as required by CalPERS policy.

We recommend that management implement procedures to track and monitor the reimbursement of real estate insurance premiums. Outstanding reimbursements should immediately be requested from the respective partnership and payments should be directed to the Cashier Unit.

**Management Response:**

Fiscal Services concurs with the recommendation. Real Estate Investment Accounting (REIA) will post all payments received for insurance premiums as a reimbursement to CalPERS from the partnership holding the real estate investment. REIA will track and monitor the reimbursement of real estate insurance premiums. REIA will work with the insurance contractor to clear any outstanding receivables due from the partners.

Payments from partnerships will be directed to the Cashiers Unit within Fiscal Services.

**Current Year Status:**

The recommendation has been implemented.

## Alternative Investments Accounting and Reporting

**Prior Year Observation #5** Alternative investment values are derived from the related partnership's financial statements as reported by PrivateEdge. During our testing, we noted two instances in which the fair values of alternative investments totaling approximately $80 million had been excluded from the year-end PrivateEdge report and the CalPERS general ledger. CalPERS staff did not discover the errors because the investment values reported by PrivateEdge were not reconciled to the underlying partnership financial statements.

We recommend that management implement procedures to ensure that alternative investments are properly valued and reported. Procedures should include reconciling PrivateEdge balances to partnership financial statements as well as evaluating the reasonableness of final valuation adjustments reflected in partnership financial statements.

**Prior Year Observation #5 (Continued)**

**Management Response:**

Fiscal Services concurs with the recommendation. CalPERS will obtain all of the necessary financial statements and reports from the Alternative Investment Partners, and will create a tracking system in order to monitor the receipt of all of the AIM partners reports. Fiscal Services will work with the Investment Office to obtain the financial statements from our partners as promptly as reasonably possible. Upon receipt of the partnerships financial statements, Fiscal Services will evaluate the reasonableness of the balances reported by Private Edge with the partnership financial statements prior to updating the general ledger accounts for year end reporting. Fiscal Services will monitor, evaluate, review, and reconcile the activity and balances of the partner's financial statements based on the quarterly activity, yearly activity and/or prior year activity to ensure that alternative investments are properly valued and reported. Fiscal Services will ensure all partnerships have had the appropriate fiscal year end accruals posted in our financial statements.

**Current Year Status:**

The recommendation has been implemented.

**Accounting for Unitization Activities**

**Prior Year Observation #6** CalPERS has elected to unitize certain investment portfolios in order to commingle the investments of the various plans. During our audit we noted several discrepancies between CalPERS' general ledger investment balances and amounts reflected in State Street Bank records. We determined that several transactions relating to the unitization of investment portfolios were erroneously posted to the general ledger, which resulted in two audit adjustments. We also noted inconsistencies in the way in which unitized and non-unitized portfolios are reported in the financial statements.

We recommend that current accounting practices be evaluated to ensure that investment activities are consistently and accurately reflected in CalPERS' financial records.

**Management Response:**

Fiscal Services concurs with the recommendation. A cross-functional project team will be established to focus on the improvement of the accounting practices for the unitization of investment portfolios. The team will review the accounting processes performed by the custodian, State Street Bank. The team will also review all associated journal entries posted in PeopleSoft and analyze the impact that it has on the financial statements. The deliverables of this project are to establish standard, repeatable, auditable and meaningful processes for the reconciliation of unitized portfolios and a consistent reporting methodology in the financial statements.

**Current Year Status:**

The recommendation has been implemented.

## RECONCILATION OF NON-INVESTMENT ACCOUNTS

### Reconciliation of Benefit Payments

**Prior Year Observation #7** Retirement benefits are processed in the Retirement Information and Benefits System (RIBS) and the Contribution Reporting System (CRS) subsidiary ledgers, and payments are disbursed by the California State Controller's Office. Fiscal Services reconciles benefit payments recorded in the CalPERS general ledger to the State Controller's Office claims schedule on a monthly basis. However, benefit payments recorded in the general ledger are not periodically reconciled to the underlying RIBS and CRS systems, which is necessary to ensure benefit payments are properly recorded as to period, amount, fund and classification.

We recommend that management implement procedures to reconcile benefit payments recorded in the general ledger to amounts reported in the respective subsidiary ledgers.

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will implement procedures to reconcile benefit payments recorded in the general ledger to the Retirement Information and Benefits System (RIBS). Fiscal Services currently reconciles all benefit payments including payments from RIBS as a part of the reconciliation between the Employer Reserve System and the general ledger. This new process will ensure that benefit payments from RIBS are recorded accurately to the respective general ledger accounts. Fiscal Services will implement this new process as a part of the mid year and annual closing for fiscal year 2007-08.

**Current Year Status:**

The recommendation has been implemented.

### Self-Funded Healthcare Premiums

**Prior Year Observation #8** Blue Cross is the third-party administrator of the self-funded PERSCare and PERSChoice heath plans. Blue Cross reconciles, on a monthly basis, premiums received from the State of California (State), along with the related enrollment records. During our testing of the PERSCare and PERSChoice premiums for the State's active and retired members, we noted the monthly premium reconciliations were not completed in a timely manner and discrepancies were not properly investigated and resolved. The May premium reconciliation was completed in October and the June reconciliation had not been completed as of the end of October. The Blue Cross premium reconciliations identified the following unresolved discrepancies:

- Members were covered under one of the plans, but were not included in participant records provided by the State; therefore, premiums were not paid.
- Members were covered and premiums were paid, but members were not included in participant records provided by the State.

**Prior Year Observation #8 (Continued)**

- Blue Cross records indicate members are covered, but CalPERS records do not indicate coverage and members were not included in participant records provided by the State.
- Payments made by the State differ from the established premiums for selected coverage.

We recommend that management establish procedures to ensure Blue Cross enrollment records are reconciled to CalPERS and State data in a timely manner. In addition, we strongly recommend that discrepancies are investigated and resolved prior to the next billing cycle or within a reasonable timeframe.

**Management Response:**

Health Benefits Branch concurs with the recommendation. The Office of Health Plan Administration (OHPA) and the Office of Employer and Member Health Services (EMHS) will develop processes to ensure that reconciliation reports will be completed timely. OHPA will work with EMHS and the Third Party Administrator (Blue Cross) to investigate and resolve discrepancies in a timely manner.

**Current Year Status:**

The prior year recommendation was not fully implemented because the June 2008 reconciliation was not completed as of November 2008.

The Office of Health Plan Administration (OHPA) and the Office of Employer and Member Health Services (EMHS) continue to emphasize the importance of this reconciliation process. Procedures for this process have been updated. In addition, management has coordinated with Anthem Blue Cross on the timing of the data contained in this report. Moving forward, Anthem Blue Cross will ensure current and accumulative data are contained in this report rather than a 90-day snapshot of the data. Management will continue to focus on ensuring discrepancies are properly investigated and resolved within a reasonable timeframe.

**INTERNAL CONTROLS OVER BENEFIT PROCESSING**

**Retiree Files**

**Prior Year Observation #9** In selecting our sample for testing Legislators' Retirement System (LRS) benefit payments, we noted nine instances in which retiree files did not contain the required documentation. Five member files did not contain the appropriate retirement application, and four files did not contain required proof of age or other documentation. In testing internal controls over the Judges' Retirement System (JRS) benefit payment process, we noted four instances in a sample of 40 of retiree files in which retirement applications could not be located and one instance in which the application was incomplete. Retirement applications include the benefit options selected by retirees as well as other key information used in the calculation of benefits. Without complete retiree files, we were unable to determine whether benefit calculations were correct.

**Prior Year Observation #9 (Continued)**

In addition, we noted retiree documents for both the LRS and JRS are not imaged in the Document Management System (DMS) in a timely manner, which increases the risk that documents will be misplaced.

We recommend the responsible department create a checklist specifying the forms and documents required for processing retirement applications. To ensure the completeness and accuracy of retiree files, staff processing retirement applications should initial each item on the checklist once the documentation has been verified and placed in the file. Supervisory personnel should independently review all retiree files to ensure documentation is complete and the checklist is signed off. In addition, retiree documents should be imaged in DMS in a timely manner, and there should be a centralized filing system for documents which have not been imaged in DMS.

**Management Response**

Member Services concurs that some documentation is missing but this is primarily in connection with the older LRS files. Member Services is updating the current policies and procedures to require that all LRS retirement files contain an LRS checklist and a new LRS calculation review form. This will ensure that receipt of all required documentation has occurred and will enable staff to validate that proper payment has been made to the member and/or beneficiary.

Member Services has revised our policies to require that all judges complete a retirement application form. Staff who process judges' retirement benefits have been notified that all judges must complete the appropriate approved retirement application form for either JRS or JRS II when applying for retirement. If a judge submits a letter in lieu of a retirement application, staff will send a retirement application form to the judge and will not complete the retirement process until the retirement application has been received. In addition, Member Services is making the retirement application available to the judges on our CalPERS website.

Regarding pre-process imaging, since JLVO does not have an automated workflow system, pre-process imaging would not be practical or efficient. As a result, all incoming documents are imaged to DMS on a post-processing basis. It is management's understanding that this issue will be resolved with the Pension System Resumption (PSR) project as all core processes, including retirement benefit and health related processes for the CalPERS, Judges' and Legislators' retirement systems will have a workflow system. In the interim, Member Services will establish a new policy requiring staff to forward the documents to DMS within two weeks following completion of the review.

Based on current staffing levels and workflow volumes, it is not feasible for supervisory personnel to review all retiree files. However, Member Services will continue to conduct a detailed post-audit review of member transactions on a routine basis. A separate staff person who is independent from the transaction processing, will conduct the post-audit review of <u>all</u> retiree files, and insure that the existing checklists are completed correctly and that all required documentation has been received.

**Current Year Status:**

The recommendation has been implemented.

## Manual Calculations

**Prior Year Observation #10** In testing internal controls over the LRS benefit payment process, we observed that LRS pension benefits are manually calculated and input into the Legislators' Monthly Roll System (LEG) subsidiary system by CalPERS staff. Such manual processes are inherently inefficient and prone to error.

We recommend that management consider automating the benefit calculation process.

**Management Response:**

Member Services agrees with this finding and will be automating the benefit calculation process in the PSR project, and the LEG subsidiary system will be replaced. In the interim, Member Services have developed a calculation review form that will contain all the information used in the calculation of the retirement benefit. Staff preparing the calculation and performing the peer review will initial the document.

**Current Year Status:**

The recommendation has been implemented.

## General Ledger Posting of Benefit Payments

**Prior Year Observation #11** In testing internal controls over the JRS benefit payment process, we noted two instances in a sample of six months in which the benefit payment claim schedules did not contain the required signature indicating the claim schedule had been reviewed and approved by appropriate supervisory personnel. Fiscal accounting utilizes the claim schedules to record benefit payments in the general ledger system. A signature on the claim schedule indicates that supervisory personnel have reviewed the amounts reported in the claim schedule for accuracy.

We recommend that Fiscal Services ensure the claims schedule has been reviewed and signed prior to posting transactions to the general ledger.

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will ensure that claim schedules are signed before posting of the information. Fiscal Services will maintain copies of the reviewed and signed claim schedules as substantiation for transactions posted to the general ledger.

**Current Year Status:**

The recommendation has been implemented.

## ACCOUNTING FOR OTHER POSTEMPLOYMENT BENEFITS

**Prior Year Observation #12** CalPERS adopted the provisions of Governmental Accounting Standards Board (GASB) Statement No. 43, *Financial Reporting for Postemployment Benefit Plans Other Than Pension Plans* (OPEB). The implementation of GASB No. 43 required CalPERS to establish two new funds. The California Employers' Retirement Benefit Trust Fund (CERBTF) was established to account for activities relating to the CalPERS prefunded OPEB plan. The Contingency Reserve Fund (CRF) agency fund was established to account for activities that were previously reported in the CRF enterprise fund. We experienced delays in the financial reporting and audit process because CRF agency fund transactions could not be easily extracted from the CalPERS general ledger.

We recommend that management should establish a process to easily identify and record CRF agency fund activities and that management should consider establishing a separate general ledger fund or sub-fund to account for these activities.

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will establish a process to easily identify and record CRF agency activity. A new process will be developed which will fulfill the objective of creating records of health premium transactions that are clearly and conveniently organized to facilitate validation and analysis by management and then by independent auditors. This new process will also produce financial statements that comply with the requirements of GASB No. 43. The new process will include transactions beginning with July 2007 and will be completed for the 2007-08 financial statements and audit.

**Current Year Status:**

The recommendation has been implemented.

## PERF ADMINISTRATIVE EXPENSE BILLINGS

**Prior Year Observation #13** During our testing of administrative expenses, we determined that charges from the Public Employees' Retirement Fund (PERF) to the CRF enterprise fund were not billed in a timely manner. PERF administrative charges for September through December 2006 were not invoiced until February 2007, and charges for February through March 2007 were not invoiced until May 2007. Timely invoicing ensures that revenues and expenses are recorded in the proper period.

We recommend that management develop and enforce policies to ensure timely billings for administrative charges between CalPERS funds.

**Management Response:**

Fiscal Services concurs with the recommendation. Fiscal Services will develop policies and procedures to ensure timely billings for administrative charges between CalPERS funds.

**Prior Year Observation #13 (Continued)**

**Current Year Status:**

The prior year recommendation for the CRF was implemented; however during the current year audit, we noted certain charges were not billed and paid timely in other funds. As such, we recommend that management develop and enforce policies to ensure timely billings for administrative charges for all CalPERS funds.

Fiscal Services concurs with the recommendation. Fiscal Services has developed and is following policies and procedures to ensure timely billings for administrative charges between CalPERS funds. CalPERS is current in its billing and recording of administrative expenses to the appropriate CalPERS funds.

## GENERAL CONTROLS - ELECTRONIC DATA PROCESSING

**Information Technology Agency Level Controls**

**Prior Year Observation #14** CalPERS policies state that all newly-hired employees will review the CalPERS Information Security Policies and Practices and sign an Information Systems Security and Confidentiality Acknowledgement (ISSACA) form. In addition, all current employees will review and re-sign the form yearly. The form states, among other items, that the employee agrees to abide by CalPERS information systems requirements including the understanding that:

- CalPERS information assets and computer resources only for CalPERS approved purposes.
- Employees are to access CalPERS systems and networks using only my assigned user identifiers and passwords.
- Employees are to notify the CalPERS Information Security Officer immediately of any actual or attempted security violations including unauthorized access; and, theft, destruction, or misuse of systems equipment, software, or data.

While CalPERS policy is that all new-hires complete and sign the ISSACA form and current employees re-sign the form yearly, we found that evidence of the signed forms are not always maintained. Our testing of 18 new-hire forms found that 17 percent could not be found. In addition, we tested six current ITSB employees and were only able to find four completed forms.

The lack of available signed forms could indicate that either the employee did not complete the review and subsequently sign the form, or that the form had been misplaced.

In either case, the evidence of completion of the form is not available putting the agency at increased risk for non-compliance to the information security policies and practices.

**Prior Year Observation #14 (Continued)**

In addition, CalPERS has performed an IT risk self-assessment documenting the organizational and management practices, personnel practices, data security practices, information integrity practices, software integrity practices, personal computer security practices, network protection practices and incident response practices. These practice areas were rated with an overall risk score derived from a probability, impact and mitigation control assessment score. The documentation was not readily available to support the effectiveness of the mitigating controls noted in the report. It is these mitigation controls that address the vulnerabilities of the agency and which should be assessed for effectiveness.

**Recommendations:**

1. CalPERS ISOF (Information Security Office) should institute new procedures to ensure that training is provided and new-hires sign the ISSACA form. Periodic internal reviews should be accomplished to ensure this is being done. In addition, procedures should be implemented to ensure that recurring training is accomplished and the recurring ISSACA form is signed and submitted to the Human Resources Department.

2. While an IT risk self-assessment has been performed and is an appropriate step in the development of a comprehensive risk assessment strategy for the agency, the ITSB Technology Services and Support Division should consider the documentation and testing of the mitigation controls noted within the current self-assessment. The effectiveness of the mitigation controls should be established and documented in order to substantiate the mitigation control score used within the risk self-assessment.

**Management Response:**

1. Management concurs with this recommendation. CalPERS Information Security Office (ISOF) has implemented an annual mandatory web-based training (WBT) program that replaces the ISSACA process. This program ensures that all staff, including civil service employees, retired annuitants and student assistants, have been informed, through the WBT, of the CalPERS information security policies and practices, and captures their acknowledgement of and agreement to abide by, the same.

   The WBT process creates a file consisting of the identity and date of everybody who has taken the training. This file is used as a compliance monitoring tool, in lieu of reviewing individual employees' personnel files looking for the most recent ISSACA forms.

   The Division Chief of the Information Technology Administration Division (ITAD) has taken the following steps to mitigate issues within the Information Technology Services Branch (ITSB):

**Prior Year Observation #14 (Continued)**

**Management Response (Continued):**

- A notice to all ITSB staff was distributed requesting an ISSACA form be reviewed and signed by all employees. ITAD staff is in the process of tracking and monitoring the forms received to ensure all forms are accounted for.

- All ITAD staff that process badge requests have been made aware and instructed to follow the policy and procedures documented in the ITSB Policy and Procedures Manual which states that a signed ISSACA form must be attached to the Badge Access Card Request form for new ITSB State employees, student assistants, retired annuitants, contractors, and consultants.

- The ITAD staff is aware that each ITSB employee is required to review and sign a form annually as stated in the ISSACA Practice. ITAD staff have developed processes to ensure each employee is instructed to review and sign a form annually as stated in the ISSACA Practice. ITAD staff will also ensure the forms are received and forwarded to Human Resources.
- In addition, ITAD will share this finding and recommendation with the CalPERS Information Security Office to ensure that all recommended actions to resolve this issue are implemented and coordinated as needed.

2. Management concurs with this recommendation. ISOF owns and oversees the CalPERS security risk assessment process. ISOF has implemented RAMP (Risk Assessment and Management Program) to assess, measure, report, recommend remediation, and track implementation of those remediation on a biennial cycle, as defined in the State Administrative Manual (SAM). RAMP consists of three main activities: 1 - structured interviews based on the RiskWatch methodology and tools; 2- document and artifact assessment; and 3- Certification and Accreditation of all new projects prior to implementation. Self-assessments, such as the one that ITSB conducted earlier this year, are not part of RAMP. Self-assessments are a good approach for an organization to take to identify and remediate issues, but do not replace the need for the independent assessment activity represented by RAMP.

**Current Year Status:**

1. The prior year recommendation is in the process of being implemented. Annual web-based training has been instituted to replace the previous ISSACA processes. Our testing in the current year found that approximately 13 percent of our sample of new hires had not completed the on-line training. Additionally, our testing of current ITSB employees found that approximately 14 percent of our sample had not accomplished their yearly refresher training. Current CalPERS standards are not specific as to the timeframe in which training will be completed for either new hires or current employees accomplishing yearly refresher training.

**Prior Year Observation #14 (Continued)**

**Current Year Status (Continued):**

The CalPERS Information Security Office (ISOF) should develop standards and procedures to ensure that new-hire web-based training is accomplished within a reasonable timeframe after an employee's start date. Likewise, the timeframe by which current employees should complete their yearly refresher training should be defined.

The Information Security Office (ISOF) will establish policies and procedures to ensure that all new employees are identified and awareness training is scheduled for them in a timely manner. The timeframe for current employees to complete the annual training will be determined. The ISOF's goal is to coordinate with the Learning Management System (initially implemented for PSR) to identify staff who have not taken the training. These policies or procedures should be completed by June 30, 2009.

2. The prior year recommendation has been implemented.

**Access to Programs and Data**

**Prior Year Observation #15** Network password configuration standards are not being enforced. The CalPERS Information Security Office has published a formal Information Security Password Practice policy, last updated in 2005. The policy defines a minimum password length and configuration standard. However, the CalPERS network is currently configured with Novell Network managing file and server access and Microsoft Active Directory managing all other network access. This dual separation of network control has resulted in the inability to electronically enforce a password configuration standard. CalPERS is aware of this inability and is currently in the process of moving all of the network control under Microsoft Active Directory. Until then, though, password configuration standards are not being electronically enforced.

While assignments to the Active Directory Domain, Schema, and Enterprise Administrative Groups are reviewed by the Windows Directory and Network Services (WNDS) manager to ensure that assignments to the groups are limited and appropriate for the employee's duties, there are no formal guidelines or policies defining who should formally have access to these Admins Groups within Active Directory. Without formal policies defining the positions and duties that would necessitate assignment to these sensitive authorization groups, it is left to personal discretion and institutional knowledge which may be subject to inconsistency depending upon who is ultimately authorizing the access.

**Prior Year Observation #15 (Continued)**

CalPERS uses an in-house application, Movaris, to manage the workflow used to authorize user account access and authorizations to the various member benefits information systems; CRS, Comet, and RIBS. A review of the process, however, finds that the designated data owners or their formal designees as reported to the Information Security Office, are not required to provide formal authorization prior to a user being allowed access to the application or data. This has the potential to increase the risk associated with the disclosure or integrity of the data as the data owner is not the final approval authority granting access.

Shared accounts are being used by the database administrators when accessing the Oracle database or the VSAM file environment. The use of these shared accounts creates a situation wherein actions taken within the database system cannot be tracked back to a specific individual. Inadvertent or malicious activity may not be able to be positively associated with a specific individual essentially eliminating an effective audit trail.

Database administrator with accounts to the Oracle database or the VSAM environments may potentially have the capability to alter member information affecting benefits payments. Tests have not been conducted to determine if the database systems have sufficient logging triggers or oversight such as file balancing or reconciliations to verify if unauthorized changes can be detected.

**Recommendations:**

1. Until the CalPERS network environment is consolidated within Microsoft Active Directory, the Information Security Office should periodically run a password cracking application to test the complexity of network passwords. Individuals who are found to have used passwords that do not adhere to the CalPERS Password Practice policy should be notified to update their passwords immediately.

2. The CalPERS WNDS manager should develop and implement formal guidelines or policy defining which positions or duties should be allowed access to the Domain, Schema, or Enterprise Admins Groups within Microsoft Active Directory. This guideline or policy should ensure that only a minimal amount of personnel are allowed access and that the access is critical to the performance of their duties.

3. The CalPERS ITSB should work to ensure that the Movaris application process includes procedures for the formal data owner or the data owner designee to provide approval prior to granting access to an application or data under the responsibility of the data owner. Current user application accounts should also be reviewed by formal data owners to ensure that all accounts currently in use have the proper approvals.

**Prior Year Observation #15 (Continued)**

**Recommendations (Continued):**

4. CalPERS ITSB should evaluate the use of shared accounts and discontinue their use where it has been determined there is a risk to the database. Database administrator accounts with schema owner access should be controlled with access granted sparingly and only after proper approval has been granted.

5. The CalPERS ISOF should conduct testing to determine if persons with schema owner access to the Oracle database or to the VSAM files can make changes to the database that would affect member benefits without detection.

**Management Response:**

1. Management concurs with this recommendation. ISOF published the Identity Authentication Practice in March 2007 to sunset the Password and Shared ID Practices. CalPERS is aware of the inability to electronically enforce all requirements outlined in the Identity Authentication Practice due to the limitations of the technology and dual network control. However, CalPERS does electronically enforce mandatory change periods, password length, password history and system lockout requirements contained in the published practice. ITSB currently has a CalPERS project to migrate the Novell Network to the Microsoft Active Directory environment which will allow for greater password compliance. At the completion of the project the WNDS Unit manager will electronically enforce all of the Identity Authentication Practice requirements where possible.

   ISOF provides awareness training and information regarding the importance of using "strong" passwords. This subject is covered at length in the annual mandatory security awareness training provided to all employees. It has been the subject of several email awareness messages published by the ISOF, the most recent of which was just three months ago. It is also covered in New Employee Orientation.

   The ISOF will consider the possibility of implementing random password cracking as a compliance tool, after a thorough analysis is completed. This analysis will include a survey of other state departments' position on the use of password cracking for compliance purposes, best business practices, and industry standards.

2. Management concurs with this recommendation. The CalPERS WNDS Unit manager and Active Directory data owner will develop and implement formal procedures defining access to the defined Administrator Groups within Active Directory in accordance with the existing published Access Control and Data Ownership ISOF Policies. This effort will be completed by January 31, 2008.

3. Management concurs with this recommendation. IT Services Branch agrees that data owner approval should be obtained prior to granting system access; however, CalPERS Senior Leadership has determined that no modifications will be made to the Movaris application.

**Prior Year Observation #15 (Continued)**

**Management Response (Continued):**

Movaris will be de-commissioned with the implementation of an Enterprise Identity and Access Management System (EIAM). EIAM will contain the data owner approval functionality.

Data owner approval is currently obtained for COMET requests through Movaris, but Movaris does not include that same functionality for RIBS and CRS. IT Services Branch is looking into the feasibility of running a monthly report of RIBS and CRS system users for the data owners to review and approve. While this process would be 'after the fact', it is a reasonable mitigation until CalPERS implements its Enterprise Identity Access Management System.

4. Management concurs with this recommendation. To address the shared accounts used to access VSAM files, Security Administration Services (SAS) will review all 'generic' and shared accounts and will work to bring them into compliance with the Identity Authentication Practice (see Observation 1.7 of the internal (FISMA) audit).

   To address shared accounts used to access Oracle databases, a single schema owner account is required by the Oracle DBMS in order to create database objects (e.g. tables, indexes, primary keys). This single owner account owns the database objects. TSSD has an operational need to allow more than one DBA to use the schema owner account and access is granted only when necessary. To mitigate the risk, the ISOF is implementing the Guardium SQL Guard appliance. This appliance provides an audit trail and is outside the control of the DBA's. Logs created by the Guardium will be routinely evaluated by the ISOF to ensure no unauthorized activities, including database schema changes, occur. The testing and implementation of the Guardium should be completed by June 2008.

5. Management concurs with this recommendation. Controls should be in place to ensure modifications to schemas and any other changes to databases are recorded in non-reputable log files. The ISOF has purchased Guardium SQL event logging appliance to address this issue. During testing of the Guardium appliance, the Information Security Office will verify that Guardium appliance flags unauthorized activities performed by the database administrators (e.g. changing member information in the database that affects benefit payments).

   The ISOF is also verifying VSAM logging processes and will expand its compliance program to include monitoring of event logs in VSAM environment to ensure timely identification of unauthorized database activities. Pending approval of the mid-year FBR, the compliance program will be in place by March 2008.

**Prior Year Observation #15 (Continued)**

**Current Year Status:**

1. The prior year recommendation is in the process of being implemented. The CalPERS project to migrate the Novell Network to the Microsoft Active Directory (AD) environment was completed in June 2008. All network accounts are now managed within Microsoft Active Directory which has the ability to enforce password configuration and expiration standards. However, the Windows Directory and Network Services (WNDS) unit is still in the process of reviewing accounts and ensuring that the password configuration standards apply to all accounts. Currently, the AD environment settings differ from the CalPERS Information Security Identity Authentication Practice in the following areas:

| Configuration | AD Settings | I.S. Identity Authentication Practice |
|---|---|---|
| Password length | 6 characters | 8 characters |
| Minimum password age | 0 | 1 day |
| Password Complexity | not required | complex passwords required |

   The CalPERS WNDS Unit should continue work on ensuring that the AD environment properly enforces account passwords in accordance with the Information Security Identity Authentication Practice.

   To implement the recommendation will require customer education and awareness. The level of effort is minimal for WNDS, however, the customer education/awareness needs to be coordinated with the Information Security Office, Enterprise Desktop Customer Support, Customer Support Center and WNDS. Implementation will be in the second quarter of calendar year 2009.

2. The prior year recommendation is in the process of being implemented. The CalPERS WNDS Unit has completed the transition from Novell Network to Microsoft Active Directory and is still in the process of establishing and configuring the Admins groups and developing the guidelines or policy to ensure that only a minimal amount of personnel are allowed access. Implementation is expected to be complete in the second quarter of calendar year 2009.

3. The prior year recommendation is in the process of being implemented. Due to financial considerations, the EIAM project has been postponed indefinitely as of the fourth quarter of calendar year 2008. Security Administration Services (SAS) is now going forward with a transition from Movaris to The Provisioning System (TPS), which was to be an interim replacement until EIAM was fully installed. The plans are now to enhance TPS with the functionality for a data owner approval process workflow. TPS is planned for initial implementation in February 2009, which will include data owner approval workflow for COMET. An enhancement to TPS, scheduled for June 2009, will incorporate data owner approval workflows for RIBS and CRS.

**Prior Year Observation #15 (Continued)**

**Current Year Status (Continued):**

As no further development has been done on the Movaris application that would ensure data owner approval prior to granting access to applications or data, the ITSB should continue efforts to implement the TPS and ensure that the automated workflow for data owner approval functions appropriately and that current user accounts are reviewed by formal data owners to ensure that all accounts currently in use have the proper approvals.

4. The prior year recommendation is in the process of being implemented. The ISOF is in the process of implementing the Guardium SQL Guard appliance to monitor database access and activity. The original implementation date of June 2008 has been pushed back and the test phase of the implementation should now be completed by December 31, 2008. At that time, a decision to implement within the production environment will be made.

5. The prior year recommendation is in the process of being implemented. The ISOF is in the process of implementing the Guardium SQL Guard appliance to monitor database access and activity. The original implementation date of June 2008 has been pushed back to the end of fiscal year 2009. To date, no testing has been completed to test for database security assurance. The ISOF has begun the Guardium SQL Guard appliance implementation. The test phase should be completed by December 31, 2008. At that time, a decision to implement into the production environment will be made.